REMARKS

Claims 1-36 are pending in this application, with claims 1, 7, 16, 17, 22, 24, 25, 26, 27, 32, 33, 34 and 35 being independent. Claims 1, 7, 16, 17, 22, 24, 25, 26, 27, 32, 33, 34 and 35 have been amended. Favorable reconsideration and allowance are respectfully requested.

The Office Action rejects claims 1, 2, 6-8, 10-12, 15 and 24 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 5,987,011 to Toh; claim 16 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,304,556 B1 to Haas; claims 25 and 26 under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,473,599 to Li; and claims 27-35 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,618,377 B1 to Miriyala. The Office Action also rejects claims 3, 4, 9 and 13 under 35 U.S. C. § 103 as obvious from Toh in view of U.S. Patent No. 6,529,515 B1 to Raz; claims 5 and 14 as obvious from Toh in view of the Applied Cryptography text by Schneier; claims 17-23 as obvious from Li in view of U.S. Patent No. 4,947,430 to Chaum; and claim 36 as obvious from Miriyala in view of U.S. Patent No. 5,968,176 to Nessett. These rejections are respectfully traversed.

Wireless ad-hoc networks exist in the art. In their present form, such networks do not rely on immobile base stations or other fixed infrastructure, and are therefore useful in military, emergency and temporary environments. Despite their many advantages, however, such networks are by their nature more vulnerable to security problems than fixed networks. In particular, with an ad-hoc network, it is possible for an "enemy" to obtain physical possession of one of the routers while it is still functioning, and manipulate the router (e.g. by reconfiguring or reprogramming it, or even by clever manipulation of its external interfaces) in such a way that the

router begins to damage the operation of the rest of the network. As will be appreciated, all routers in a network must trust each other in order for the network to function properly, and such trust breaks down when one of the routers has been seized.

The present invention solves this problem, by applying special, inventive techniques when it is determined that a functioning router in the network has become compromised. For example, in accordance with the present invention as recited in claim 1, a router in the network evaluates a excise signal indicating that the network control computer has determined that another functioning router has become compromised, determines the authenticity of the excise signal, and when the excising signal is authenticated excises the compromised router and reroutes the excise signal to yet another router.

Independent claims 7, 16, 17, 22, 24, 25, 26, 27, 32, 33, 34 and 35 are directed to other embodiments of the present invention. In all of those claims, when it is determined that a functioning router in the network has become compromised, the compromised router is excised or cut-off from the network, or messages sent by the compromised router are disregarded.

None of the prior art teaches or suggests these salient features. To the contrary, and as set forth in greater detail below, the primary references applied by the Office Action do not deal with a functioning but compromised router at all. Instead, they deal only with finding an optimal path through the network, or with maintaining network connectivity when a router in the network is not functioning at all.

Toh is directed to a routing method for ad-hoc mobile communication networks, in which the stability of routes through the network is measured using an associativity

characteristics, and in which the selection of a particular route for transmission of information is based upon that particular route's stability. The associativity characteristic itself is measured by each mobile host periodically transmitting and receiving identifier beacons (called "ticks" in the parlance of Toh) and updating the status of the corresponding links. A mobile host is said to exhibit a high state of mobility when it has a low number of associativity ticks with its neighbors, and a low state of mobility when it has a high number of ticks. Hosts exhibiting low mobility are considered to be ideal for routing. But the high mobility routers in Toh are not deemed to be functioning routers that have become compromised, and are not excised from the network or disregarded. Instead, they are merely deemed to be less than ideal for routing.

Haas deals with routing and mobility management protocols for ad-hoc networks. Haas describes a mobility management protocol in which a node needing a router consults its associated Mobility Reporting Center (MRC). The MRC locates the destination node by sending a request within a virtual MRC subnet to the other MRCs, and the MRC that covers the destination responds. A spine route is then created that routes the message from the source node to the source's MRC to destination's MRC to the destination. Then, other nodes that are in the direction of the spine route are queried, to determine if there is a more optional route available. As is the case with Toh, however, the Haas technique is simply looking to find a better route, and is not looking to determine that functioning nodes have become compromised, or to excise or disregard such nodes.

Li is directed to a routing protocol in which active routers are backed-up by stand-by routers. When a standby router detects that an active router has failed (due to power failure, a

rebooting operation, a maintenance activity or the like), it takes over for the failed active router, by taking over the active router's media access control (MAC) and Internet protocol (IP). The failed router of Li are not functioning routers that have become compromised, but are instead routers that have become inoperative. The issue is not to excise or disregard the inoperative router, but rather to put an operative one in its place.

Miriyala, like Li, is also concerned with providing stand-by capabilities, to reduce the likelihood of network transmission failures due to the unavailability of a network device. Towards that end, redundant asynchronous transfer mode (ATM) devices are provided, such that if one device breaks down, a stand-by device is utilized. As is the case with Li, Miriyala has nothing at all to do with functional but compromised routers.

Raz simply shows, in a computer network environment, that multiple levels of security may be provided via authentication and session classification. It does not even relate to an ad-hoc wireless network, and certainly does not teach or suggest techniques for handling functioning but compromised routers. Schneier is cited by the Office Action for teaching the benefits of public key encryption, Chaun for teaching the use of digital signatures and Nessett for teaching firewall technologies. These documents, similarly, teach nothing concerning functioning but compromised routers, and do not correct the deficiencies of any of the references discussed above.

Accordingly, Applicant respectfully submits that none of independent claims 1, 7, 16-17, 22, 24-27 or 32-35 are anticipated or rendered obvious by Toh, Haas, Li, Miriyala, Raz,

Schneier, Chaun or Nessett – or any combination of them – and respectfully request the Examiner to remove the Section 102 and 103 rejections.

The remaining claims all depend from one of the independent claims, and each partakes in the novelty and non-obviousness of its respective base claims. The dependent claims also recite additional patentable features of the present invention, and individual reconsideration and allowance of each are respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, Applicant respectfully requests favorable reconsideration and passage to issue of the present application.

If there are any fees due in connection with the filing of this response, please charge the fees to our Deposit Account No. 18-1945. If an extension of time under 37 C.F.R. § 1.136 not accounted for above is required, such an extension is requested and the fee should also be charged to our Deposit Account.

Respectfully Submitted,

Date: May 13, 2004

Edward A. Gordon
Registration No.: 54,130

ROPES & GRAY LLP
One International Place
Boston, Massachusetts 02110-2624
(617) 951-7000
(617) 951-7050 (Fax)
Attorneys/Agents For Applicant